



# UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE  
United States Patent and Trademark Office  
Address: COMMISSIONER FOR PATENTS  
P.O. Box 1450  
Alexandria, Virginia 22313-1450  
www.uspto.gov

| APPLICATION NO. | FILING DATE | FIRST NAMED INVENTOR | ATTORNEY DOCKET NO. | CONFIRMATION NO. |
|-----------------|-------------|----------------------|---------------------|------------------|
| 09/829,074      | 04/09/2001  | Robert W. Baldwin    | 155607-0351         | 7424             |

7590 12/21/2004

LOREN H. McROSS  
PHOENIX TECHNOLOGIES LTD.  
915 MURPHY RANCH ROAD  
MILPITAS, CA 95035

EXAMINER

SON, LINH L D

| ART UNIT | PAPER NUMBER |
|----------|--------------|
|----------|--------------|

2135

DATE MAILED: 12/21/2004

Please find below and/or attached an Office communication concerning this application or proceeding.

|                              |                        |                     |  |
|------------------------------|------------------------|---------------------|--|
| <b>Office Action Summary</b> | <b>Applicati n No.</b> | <b>Applicant(s)</b> |  |
|                              | 09/829,074             | BALDWIN ET AL.      |  |
|                              | <b>Examiner</b>        | <b>Art Unit</b>     |  |
|                              | Linh Son               | 2135                |  |

-- The MAILING DATE f this communication appears on the c ver sheet with the correspondence address --  
**Period f r Reply**

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

#### Status

- 1) ☒ Responsive to communication(s) filed on 09 April 2001.
- 2a) ☐ This action is **FINAL**.                      2b) ☒ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

#### Disposition of Claims

- 4) ☒ Claim(s) 1-47 is/are pending in the application.
- 4a) Of the above claim(s) \_\_\_\_\_ is/are withdrawn from consideration.
- 5) ☐ Claim(s) \_\_\_\_\_ is/are allowed.
- 6) ☒ Claim(s) 1-47 is/are rejected.
- 7) ☐ Claim(s) \_\_\_\_\_ is/are objected to.
- 8) ☐ Claim(s) \_\_\_\_\_ are subject to restriction and/or election requirement.

#### Application Papers

- 9) ☐ The specification is objected to by the Examiner.
- 10) ☐ The drawing(s) filed on \_\_\_\_\_ is/are: a) ☐ accepted or b) ☐ objected to by the Examiner.  
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).  
Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

#### Priority under 35 U.S.C. § 119

- 12) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) ☐ All    b) ☐ Some \* c) ☐ None of:
1. ☐ Certified copies of the priority documents have been received.
2. ☐ Certified copies of the priority documents have been received in Application No. \_\_\_\_\_.
3. ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

\* See the attached detailed Office action for a list of the certified copies not received.

#### Attachment(s)

- |  |   |
|--|---|
| 1) <input checked="" type="checkbox"/> Notice of References Cited (PTO-892)  | 4) <input type="checkbox"/> Interview Summary (PTO-413)<br>Paper No(s)/Mail Date. _____ |
| 2) <input type="checkbox"/> Notice of Draftsperson's Patent Drawing Review (PTO-948)                                   | 5) <input type="checkbox"/> Notice of Informal Patent Application (PTO-152)             |
| 3) <input type="checkbox"/> Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08)<br>Paper No(s)/Mail Date _____ | 6) <input type="checkbox"/> Other: _____  |

## DETAILED ACTION

### *Claim Rejections - 35 USC § 102*

1. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

A person shall be entitled to a patent unless –

(e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

2. Claims 10-40, and 42-47 are rejected under 35 U.S.C. 102(e) as being anticipated by England et al, US Patent No. 6327652B1, hereinafter '652.
3. As per claims 10 and 26, "a method of controlling read and write access to data to an application by restricting the availability of a cryptographic key to an application, the method comprising: a first key; an application container that holds a sealed or unsealed form of the data that the application wants to access" is taught in '652 (Col 17 lines 1-58); "a cryptographic gate keeping module that performs a cryptographic digest of a portion of the bytes that make up the calling application to compute a cryptographic digest" is taught in '652 (Col 17 lines 1-30); and "a cryptographic processing module that includes integrity-checking that examines the application container and cryptographic digest, and the first key to

determine if the application is allowed to unseal the data in the given application container, or when sealing the data modifies it to add the integrity check information" is taught in '652 (Col 17 lines 33-60).

4. As per claim 11, "the method recited in claim 10 wherein a privacy method performed by the cryptographic processing module that decrypts the data in the application container using a key derived from at least the first key and cryptographic digest" is taught in '652 (Col 17 lines 33-57).
5. As per claim 12, "the method recited in claim 10 further including a privacy method performed by the cryptographic processing module that encrypts the data in the application container using a key derived from at least the first key and cryptographic digest" is taught in '652 (Col 17 lines 33-57).
6. As per claim 13, "the method recited in claim 12 wherein the privacy method adds to the application container the cryptographic digest before the encryption is performed" is taught in '652 (Col 17 lines 33-57).
7. As per claim 14, "a method of controlling access to data to an application by restricting the availability of a cryptographic key to the application on a specific device, comprising: a key known to a cryptographic processing module" is taught in '652 (Col 17 lines 1-15); "an application container data structure that contains

a cryptographically sealed form of the data that the application wants to access” is taught in ‘652 (Col 17 lines 47-54); “a cryptographic gate keeping function that intercepts all access between application-level programs and the cryptographic processing module” is taught in ‘652 (Col 17 lines 1-15); “includes a means to examine a portion of the bytes of an executable in-memory image of a program that is attempting to access cryptographic services or data; and computes a cryptographic digest of a portion of the bytes of in-memory image of the calling application to compute the cryptographic digest of the application” is taught in ‘652 (Col 13 lines 20-35); and “an integrity-check method performed by the cryptographic processing module that examines the application container data structure and cryptographic digest, and the first key to determine if the application is allowed to unseal the data in the given application container data structure, or when sealing the data modifies it to add the integrity check information” is taught in ‘652 (Col 13 line 60 to Col 14 line 32, Col 15 lines 30-46, and Col 17 lines 1-58) .

8. As per claim 15, “the method recited in claim 14 further comprising a privacy method performed by the cryptographic processing module that encrypts or decrypts the data in the application container data structure using a key derived from at least the first key and cryptographic digest and when data is encrypted it optionally adds to the application container data structure the cryptographic digest before the encryption is performed” is taught in ‘652 (Col 15 lines 30-45,

and Col 17 lines 1-58).

9. As per claim 16, “the method recited in claim 14 wherein the cryptographic gate keeping function is concurrently or previously given an authorization buffer that specifies the allowed operations for the application and the cryptographic gate keeping function confirms that the request operation is allowed” is taught in ‘652 (Col 13 line 60 to Col 14 line 32, Col 15 lines 30-46, and Col 17 lines 1-58).
10. As per claims 17 and 28-30, “the method recited in claims 14 wherein the integrity-check method includes the steps of deriving a cryptographic variable from the cryptographic digest and the first key, and using the cryptographic variable to check a message authentication code that is stored in the application container data structure” is taught in ‘652 (Col 13 line 60 to Col 14 line 32, Col 15 lines 30-46, and Col 17 lines 1-58).
11. As per claims 18, 31, 33, and 35, “the method recited in claims 14 wherein the integrity-check method includes decrypting a portion of the application container data structure using a key derived from the first key to create a resulting value to data derived from the cryptographic digest, and allowing the access to the cryptographically sealed from of the data if the resulting value is the same as the data derived from the cryptographic digest” is taught in ‘652 (Col 13 line 60 to Col

14 line 32, Col 15 lines 30-46, and Col 17 lines 1-58).

12. As per claim 19, "the method recited in claims 14 wherein the privacy step includes the steps of deriving a cryptographic variable from the cryptographic digest and the first key and optionally other information, or of deriving a second cryptographic variable from the cryptographic digest and the first key and a cryptographic variable chosen by a component of an application and optionally other information, and this derived key is used to decrypt or encrypt a portion of the application container data structure" is taught in '652 (Col 13 line 60 to Col 14 line 32, Col 15 lines 30-46, and Col 17 lines 1-58).
13. As per claim 20, "the method recited in claim 19 wherein the cryptographic variable is derived with one or more applications of a hash function by concatenating dependant values in a particular order" is taught in '652 (Col 13 lines 25-40, and Col 14 lines 8-38).
14. As per claim 21, "the method recited in claims 14 wherein a portion of the cryptographic processing module executes during an system management interrupt" is taught in '652 (Col 13 line 60 to Col 14 line 8).
15. As per claim 22, "a method for authenticating an identified application on an identified device to another computing machine comprising an authentication

server with the help of another computing machine comprising a device authority, the method comprising: performing a first cryptographic enrollment operation during a system management interruption on the identified device producing a result that is sent to the device authority; performing a second cryptographic enrollment operation during the system management interruption on the identified device processing a value generated by the device authority that is received by the identified device” is taught in ‘652 (Col 9 line 42 to Col 10 lines 63, and Col 13 lines 37-60); “performing a first cryptographic registration operation during the system management interruption on the identified device producing a result that is sent to the authentication server; performing a second cryptographic registration operation by the authentication server producing a cryptographic variable that is stored for use during the authentication method” is taught in ‘652 (Col 9 line 42 to Col 10 lines 63, and Col 13 lines 37-60); “performing a first cryptographic authentication operation during the system management interruption on the identified device producing authentication data that is sent to the authentication server and performing a second authentication cryptographic operation by the authentication server on the authentication data received from the identified device using at least the cryptographic variable to determine the result of the authentication” is taught in ‘652 (Col 9 line 42 to Col 10 lines 63, and Col 13 lines 37-60).



16. As per claim 23, "a method for authenticating an identified application program on an identified device, or for providing a second factor for identifying a user of the identified device to another computing machine comprising an authentication server, the method comprising: performs an enrollment process including communication with a device authority and an authentication server to create an application container data structure on the device, wherein the application container data structure is cryptographically associated with the application program" is taught in '652 (Col 9 line 42 to Col 10 lines 63, and Col 13 lines 37-60); "storing credential information, and wherein the authentication server stores a cryptographic variable for the application container data structure" is taught in '652 (Col 9 lines 42-51); "unsealing the application container data structure that stores the credentials" is taught in '652 (Col 10 lines 14-25); "modifying the credentials; resealing the application container data structure, wherein at least part of said resealing occurs during an SMI on the same CPU that executes the code of the application program" is taught in '652 (Col 12 lines 8-35); "sending identifying information and at least a portion of the resealed Application Container data structure to the authentication server" is taught in '652 (Col 12 line 50 to Col 13 line 9); "receives the identifying information and the data derived from the application container data structure; using the identifying information to lookup or compute a cryptographic variable to unseal the application container data structure" is taught in '652 (Col 13 lines 10-59) ; "authenticating the identified application program and the identified device if the unsealed application

container includes acceptable values; and storing a key associated with the application container data structure” is taught in ‘652 (Col 13 line 60 to Col 14 line 40, and Col 16 lines 60-67).

17. As per claims 24, 38, 42-43, and 47, “a method for creating and utilizing one or more virtual tokens on a device for the purpose of authentication, privacy, integrity, authorization, auditing, or digital rights management, the method comprising: an application program for each of said corresponding type of virtual token; an application container for each of said virtual tokens” is taught in ‘652 (Col 14 lines 9-33); “a cryptographic gate keeping component that computes an cryptographic digest of calling application that is requesting cryptographic services of a cryptographic processing component; wherein the cryptographic processing component is accessed via the cryptographic gate keeping component, wherein the cryptographic processing component knows a first key and a public key, wherein the cryptographic processing component performs cryptographic sealing and unsealing of application container data structures, where a portion of the cryptographic operations are performed during a system management interrupt” is taught in ‘652 (Col 9 line 42 to Col 10 lines 63, and Col 13 lines 37-60), “wherein the cryptographic processing component checks the integrity of the calling application by checking a digital signature of a portion of the application's code or static data, using a public key that has been loaded into the cryptographic processing component and a cryptographic digest value,

wherein the cryptographic digest value includes a recently computed cryptographic hash of a portion of the calling application's in-memory image" " is taught in '652 (Col 9 line 42 to Col 10 lines 63, and Col 13 lines 37-60), "wherein the cryptographic gatekeeping and cryptographic processing component a) derive a key for unsealing the application container data structure from the first key and cryptographic digest, b) use the derived key to check the message authentication code on the application container data structure, and returns an error if the message authentication code is correct, and c) use the derived key to decrypt the data in the application container data structure and return it to the application" is taught in '652 (Col 9 line 42 to Col 10 lines 63, Col 13 lines 37-60, and Col 17 lines 1-58).

18. As per claims 25 and 39-40, "a method of securely associating a private key with an application program associated with a device, comprising: creating an application container that contains private keys secured by a key associated with the application program and the device" is taught in '652 (Col 9 line 42 to Col 10 lines 63, and Col 13 lines 37-60).
19. As per claim 27, "the system of claim 26, wherein the application program is part of an operating system kernel" is taught in '652 (Col 8 lines 25-37).

20. As per claims 32, and 45, "the method of claim 26, wherein the cryptographic key is derived from a plurality of data items chosen from the group consisting of; the first key; the cryptographic digest; a password; and value passed to the cryptographic gatekeeping function" is taught in '652 (Col 17 lines 1-30).
21. As per claim 34, "an enhanced computing device, comprised of: a processor to execute a plurality of application programs in a normal mode; a security kernel that executes in a restricted mode; a key that is accessible by the security kernel when said processor is executing in the restricted mode, where the security kernel used the key to authenticate an application program on the computing device and provides cryptographically secure data for use by the application program" is taught in '652 (Col 3 lines 1-20, Col 9 lines 41-67).
22. As per claim 36, "the enhance computing device of claim 35, wherein the cryptographically secure data will not be accessible when moved to a different device" is taught in '652 (Col 7 line 45 to Col 8 line 37).
23. As per claims 37 and 47, "the enhance computing device of claims 35 and 34, wherein the container will not function properly when moved to a different device" is taught in '652 (Col 12 lines 53-65).

24. As per claim 44, " the system of claim 14, wherein the normal operating mode is one of a kernel mode and a user mode in a 32-bit operating system environment" is taught in '652 (Col 16 lines 1-14, and Col 17 line 60 to Col 18 line 15).

***Claim Rejections - 35 USC § 103***

25. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

26. Claims 1-9, and 41 are rejected under 35 U.S.C. 103(a) as being unpatentable over England et al, US Patent No. 6327652B1, hereinafter '652.
27. As per claims 1 and 9, "a system for using and protecting access to a master cryptographic key, comprising: non-volatile storage; a system initialization process that: reads the first key from the non-volatile storage during a system initialization process" is taught in '652 (Col 3 lines 15-20, and Col 13 lines 60-65); "writes a sensitive value derived from the first key to a hidden storage location" is taught in '652 (Col 8 lines 7-37, Col 12 lines 53-65, Col 13 line 60 to Col 14 line 32); "means to prevent access to the hidden storage location by programs running in the normal operating mode of the system" is taught in '652 (Col 16

lines 50-67); and “means to allow access to the hidden storage location by a program running in a restricted operating mode of the system” is taught in ‘652 (Col 17 lines 1-58). However, “the disabling access to the non-volatile storage by any program running in the system until the next start of system initialization process” is not specifically explained in ‘652. Nevertheless, the system does teach steps of booting up the device securely using the boot loader which the only time reading the information from the nonvolatile memory (Smart card) and after deriving the necessary sensitive information from the non-volatile memory the boot loader relinquishes the control to the boot block (Col 3 lines 1-20, and Col 13 line 60 to Col 14 line 8). Therefore, it is obvious at the time of the invention was made for one having ordinary skill in the art to realize that the steps of disabling access to the non-volatile storage until the next system initialization is included in the system to protect secrecy of the device (Col 3 lines 1-13).

28. As per claim 2, “the system recited in claim 1 wherein the sensitive data is the first key” is taught in ‘652 (Col 15 lines 30-40).
29. As per claim 3, “the system recited in claim 1 wherein the sensitive data is derived from the first key” is taught in ‘652 (Col 13 line 60 to Col 14 line 40).

30. As per claim 4, "the system recited in claim 3 wherein the sensitive data is a second key retrieved from encrypted data stored on disk, where the stored data is encrypted with the first key" is taught in '652 (Col 14 lines 1-8).
31. As per claim 5, "the system recited in claim 1 wherein software in BIOS ROM controls the system during the system initialization process that begins in response to a power-on or reset signal" is taught in '652 (Col 6 lines 9-23).
32. As per claim 6, "the system recited in claim 1" is taught in '652. However, "the non-volatile storage is non-volatile random access memory with read and write access controlled by a latch; the latch is opened at the start of system initialization process due to a hardware function responding to a power-on or reset event, thereby enabling system access to the non-volatile random access memory; and the latch is closed during the system initialization process, thereby denying system access to the non-volatile random access memory until the next start of system initialization" is not specially taught in '652. Nevertheless, the secure processor device includes steps to load the application container in which the information read from the secure area of the CPU to authenticate and create a highly trusted application environment to download the content only be done once at boot-up. The same information is not needed until the next power-up (Col 3 lines 1-14, and Col 9 line 40 to Col 10 line 63). Therefore, it is obvious at the time of the invention was made for one having ordinary skill in the art to

realize the safety features claimed are also considered in '652 to provide a secure and protective environment for the content provider.

33. As per claims 7 and 8, "the system recited in claims 1 wherein the hidden storage is system management memory which is not accessible by any program running in the normal operating mode of the system; the restricted operating mode is a System Management Mode in which access to system management memory is permitted; and the restricted operating mode is controlled by a CPU protection ring reserved for use by operating system" taught in '652 (Col 16 lines 50-67). However, the hidden secure storage is not specifically taught as the Random Access Memory (RAM) in '652. Nevertheless, it is obvious for one having ordinary skill in the art at the time of the invention was made to realize that RAM is a great location to store secret information since it is only access-able through the operating system (Col 16 lines 50-67).

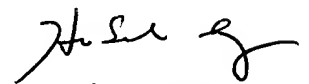
34. As per claim 41, " the system of claim 14, wherein the normal operating mode is one of a kernel mode and a user mode in a 32-bit operating system environment" is taught in '652 (Col 16 lines 1-14, and Col 17 line 60 to Col 18 line 15).

### **Conclusion**

35. Any inquiry concerning this communication from the examiner should be directed to Linh Son whose telephone number is (571)-271-3856.



36. If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor Kim Y. Vu can be reached at (571)-272-3859. The fax numbers for this group are (703)-872-9306 (official fax). Any inquiry of general nature or relating to the status of this application or proceeding should be directed to the group receptionist whose telephone number is (571)-272-2100.
37. Information regarding the status of an application may be obtained from the Patent Application Information Retrieval IPAIR.I system. Status information for published applications may be obtained from either Private PMR or Public PMR. Status information for unpublished applications is available through Private PMR only. For more information about the PAIR system, see <http://pzr-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

  
AV 2135

**Linh LD Son**

**Patent Examiner**